Myndigheten för samhällsskydd och beredskap

Årsrapport it-incidentrapportering 2019

Vad har hänt, varför har det hänt, och vad ska göras för att undvika att det händer igen?

Årsrapport it-incidentrapportering 2019 – Vad har hänt, varför har det hänt, och vad ska göras för att undvika att det händer igen?

Foto: Shutterstock
Tryck: DanagårdLiTHO
Produktion: Advant

Publikationsnummer: MSB1526 - april 2020
ISBN: 978-91-7927-027-8

Förord

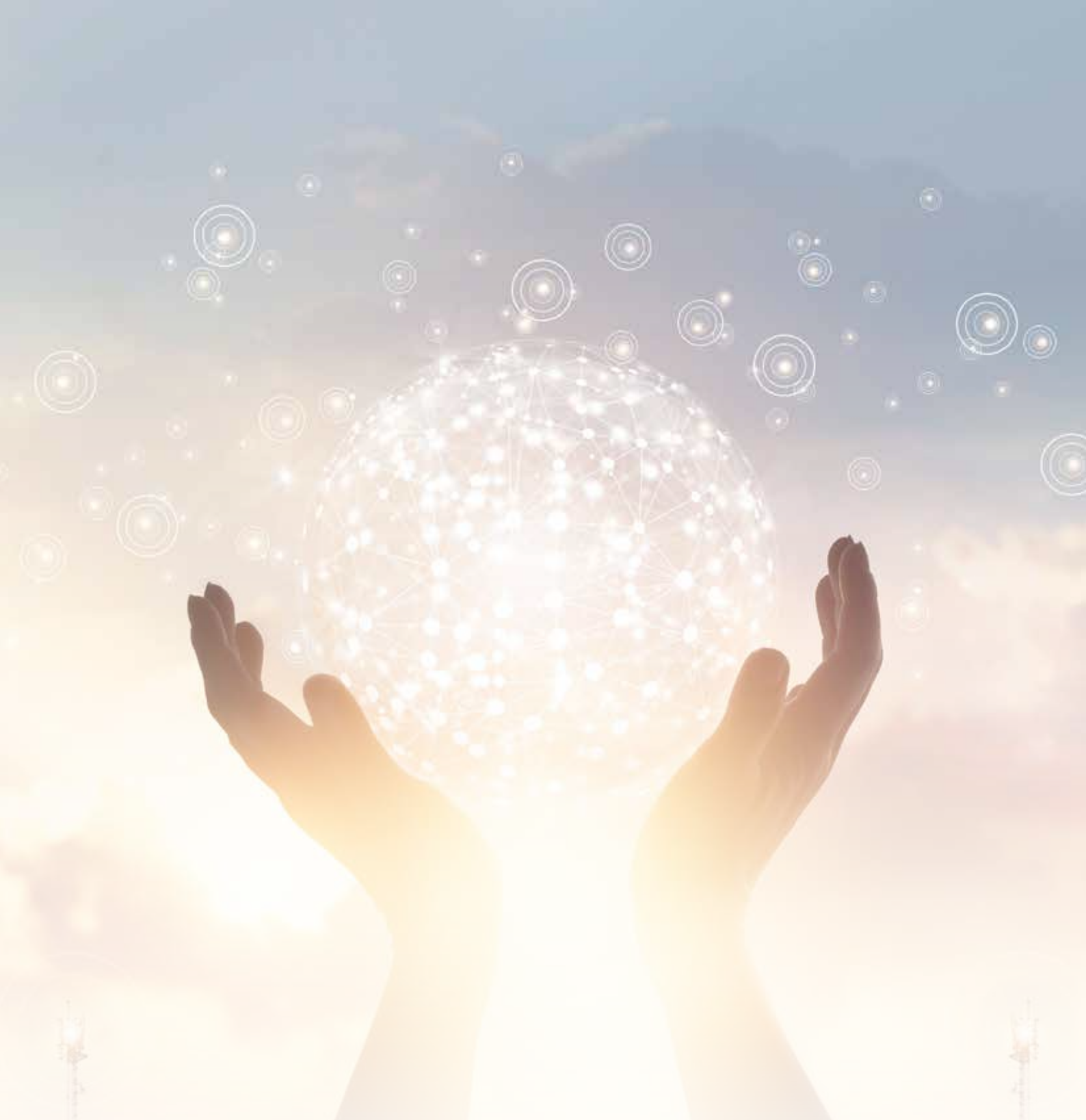
Samhället digitaliseras i hög takt, tjänster som förut tillhandahölls analogt erbjuds nu digitalt. Det skapas utöver det även tjänster som inte har någon analog förebild. Denna utveckling accelererar i takt med att teknikens möjligheter flyttas fram samt att medborgarnas förväntningar på vilken service som ska erbjudas digitalt ökar. Digitaliseringen i kombination med förväntningar skapar en situation där hastighet och förändringsdriv går före säkerhet och kontroll. I denna verklighet befinner sig samtliga svenska myndigheter. Alla behöver balansera det innovativa och nya med det systematiska riskbaserade, en balansgång som kan avgöra hur väl rustade svenska myndigheter och i förlängningen det svenska samhället är då it-incidenter inträffar.

Det är naivt att tro att it-incidenter är en företeelse som kan arbetas bort. Det kommer alltid att inträffa incidenter, det är hur väl organisationer, såväl offentliga som privata, hanterar de inträffade incidenterna som avgör hur allvarliga konsekvenserna blir. Det är inte aktuellt att tala om någon nollvision för allvarliga it-incidenter. Området är alldeles för komplext och beroendena för stora. Det är däremot rimligt och önskvärt att arbeta för en nollvision rörande de incidenter som skapar stora konsekvenser på grund av ett undermåligt informations- och cybersäkerhetsarbete. MSB erbjuder stöd i olika former under informationens hela livscykel och det är vår uttalade vilja att det förebyggande, systematiska och riskbaserade informationssäkerhetsarbetet ges den uppmärksamhet och de resurser som krävs för att minska antalet allvarliga konsekvenser när något går fel.

Det vi myndigheter har att erbjuda samhället är beroende av att medborgarna litar på att myndigheterna utför sina uppdrag på ett säkert och effektivt sätt. Om tilliten till statliga myndigheter tillåts erodera på grund av ett bristfälligt säkerhetsarbete i kombination med en hastig och expansiv digitalisering riskerar vi att skada den så viktiga tilliten som skapar legitimitet för myndigheternas verksamhet.

Åke Holmgren
Chef avdelningen för cybersäkerhet
och säkra kommunikationer
Myndigheten för samhällsskydd och beredskap

Innehåll



Sammanfattning

Sammanfattning

MSB har sedan april 2016 mottagit rapporter om allvarliga it-incidenter från statliga myndigheter. Sedan dess har samhällets digitalisering fortsatt och i vissa avseenden ökat takten. Denna årliga rapport tar sitt avstamp i de rapporter som MSB tar del av samt den övriga omvärldsbevakning och övriga inflöden. Samtliga myndigheter behöver förhålla sig till krav på att digitalisera delar av eller hela sin verksamhet. Dessa kommer såväl från politiskt håll i och med krav på ökad effektivitet, som från medborgare i form av ökade förväntningar på tillgänglighet och service via exempelvis applikationer i smarta telefoner. Denna utveckling innebär en utmaning för hela samhället. För att på ett ändamålsenligt sätt digitalisera sin verksamhet behövs förebyggande säkerhetsarbete. Dessvärre är det ofta ny teknik ligger ett eller flera steg framför säkerhetsarbetet generellt, och säkerhetsarbetet hos myndigheter specifikt. Denna diskrepans är inte ny och MSB har i tidigare rapporter och presentationer pekat på den ökande säkerhetsskuld som ligger till grund för många av de allvarliga it-incidenter som rapporteras.

I rapporten finns ett antal lärande exempel på allvarliga it-incidenter som bygger på rapporteringen under 2019. Vi hoppas att dessa exempel och tillhörande åtgärdsförslag kan användas i myndigheternas förebyggande arbete. De kompletterar de föreskrifter och vägledningar som MSB i övrigt har tagit fram för att stötta myndigheterna i deras systematiska och riskbaserade informations- och cybersäkerhetsarbete. Många myndigheter drabbas av liknande it-incidenter som beskrivs, ofta i onödan, då det finns enkla sätt att förebygga de flesta av dem, alternativt att minska konsekvenserna när de inträffar. Denna rapport är även en vägledning för de myndigheter som omfattas av rapporteringsplikten. Med grund i den samlade kunskapen om vilka incidenter som inträffar ger rapporten rekommendationer om relevanta säkerhetsåtgärder. Vägledningen och rekommendationerna är giltiga för övriga verksamheter i samhället utöver rapporteringsskyldiga myndigheter. Kommuner, regioner eller privata företag kan även de ta stöd i den vägledning som denna rapport ger.

Under 2019 mottog MSB 296 rapporter om allvarliga it-incidenter från statliga myndigheter. En analys av de rapporterade incidenterna visar att:

- Handhavandefel har ökat.
- Fler myndigheter rapporterar allvarliga it-incidenter men antalet rapporter är fortsatt lågt.
- Systematiskt och riskbaserat informationssäkerhetsarbete med incidenthanteringsprocesser och kontinuitetsplanering skulle höja lägstanivån.

Digitaliseringen av samhället

1. Digitaliseringen av samhället

Samhället är idag ihop- och uppkopplat och att koppla samman verksamheter och aktörer är en av grundidéerna med att digitalisera. Målet är att skapa mervärden och möjliggör effektivisering av processer. Sammankopplingen resulterar i beroenden som är svåra att kartlägga och redogöra för. Beroenden är ofrånkomliga och behöver inte vara ett problem, men de beroenden som organisationen inte vet om kan på sikt ge oöverblickbara konsekvenser. Komplexiteten i digitaliseringen blir på detta sätt en sårbarhet i sig själv. De beroenden som byggs upp kan ses som en kedja där kedjan inte är starkare än den svagaste länken. För att minska riskerna för allvarliga konsekvenser behöver dessa svaga länkar bli starkare. Inte minst med avseende på att det finns en hotbild mot svenska myndigheter.[1] Men allvarliga it-incidenter kan också ske utifrån rena misstag och triviala fel.

Samhället digitaliseras i hög takt. Utvecklingen mot effektivare och snabbare hantering av såväl myndighetsuppgifter som privata ärenden driver på från flera håll och skapar situationer där eftertänksamhet och systematiskt säkerhetsarbete i vissa fall får stryka på foten med argument som exempelvis att det försenar utvecklingen. Denna utveckling är inte ny, det som är nytt är den hastighet med vilken nya innovationer integreras i verksamhetsprocesser. Tidigare har digitalisering typiskt varit ett fenomen där en avgränsad del av en verksamhet görs digital, med en analog förebild. Detta innebär att det finns en förlaga, och något att relatera till, samt falla tillbaka på då den digitala versionen inte fungerar. I och med den snabba och ständigt accelererande teknikutvecklingen börjar denna modell för digitalisering utmanas. Numera skapas nya processer och verksamheter som är byggda enbart för den digitala verkligheten. Ytterligare problematiserande aspekter för den snabba digitaliseringen är det faktum att många av de system som myndigheter använder dagligdags för sin informationshantering är gamla, och i många fall så pass gamla att det i sig är en säkerhetsrisk. Riksrevisionen har påtalat detta problem och kommit till slutsatsen att det hotar informationssäkerheten hos statliga myndigheter att it-system och it-miljöer är föråldrade. I vissa fall är de så komplexa att det är svårt, eller till och med omöjligt, att få en överblick över hur systemet är ihopkopplat eller vilka system som är beroende av varandra för att fungera.[2] Ytterligare aspekter som fördjupar den problembild som Riksrevisionen pekar på, och som MSB delar, är det faktum att flera av de stora myndigheterna agerar värdmyndigheter åt mindre myndigheter när det gäller it-drift.

1. Se exempelvis FRA:s årsbok 2019, Musts årsöversikt 2019 samt Säkerhetspolisens årsbok 2019.
2. RiR 2019:28

Denna utveckling, som i grund och botten handlar om effektivisering och hushållning med skattemedel, riskerar att äventyra säkerheten hos flera aktörer om det är så att föråldrade och komplexa system härbärgerar flera myndigheters information. Ett antal centrala myndigheter är till sin natur centrala informationsnoder för mycket verksamhet i samhället. Dessa noder är vitala för att hela samhällets tillgång till data ska säkerställas.

Det pågår för närvarande en rad initiativ för att digitalisera staten. I detta arbete ingår att strukturera, tillgängliggöra, och vidareutnyttja centrala datamängder. Utöver detta pågår arbete med att bygga gemensamma it-infrastrukturer för informationsutbyten. Användandet av molntjänster och outsourcad it-drift är redan en realitet för många myndigheter. Detta ställer oundvikligen högre krav på det systematiska informationssäkerhetsarbetet både inom och mellan organisationer samt en kraftsamling kring gemensamma cybersäkerhetsfrågor på samhällsnivå. I ett framtida läge där mycket av det dagliga informationsutbytet myndighet till myndighet och myndighet till privatperson förväntas kunna ske genom alltmer sammanflätade infrastrukturer för informationsutbyte kan avbrott, oriktig hantering av information eller informationsläckage få omfattande konsekvenser för exempelvis handläggning, rättssäkerhet, privatpersoners ekonomiska trygghet och samhällets säkerhet och beredskapsförmåga. När större datavolymer på sikt ska kunna nås av fler krävs en väl genomtänkt infrastruktur för behörighetskontroll, autentisering och uppföljning. Behörighetskontroll med stöd av digitala identiteter kommer bli en alltmer kritisk del av ett säkert digitaliserat samhälle som ska kunna skyddas mot identitets- och informationsstölder.

I de kommande årens arbete med att fortsätta digitaliseringen av myndigheternas informationshantering kommer ekonomiska incitament för effektivisering och kostnadsbesparingar att vara starka drivkrafter. I takt med att nya digitaliserade lösningar integreras med äldre it-lösningar som i sitt ursprung inte dimensionerats uppstår stora utmaningar för informationssäkerheten.

Arbetet för ett säkrare digitalt samhälle

2. Arbetet för ett säkrare digitalt samhälle

MSB:s arbete med informations- och cybersäkerhet omfattar hela hotskalan, det vill säga allt ifrån exempelvis naturhändelser som påverkar informations- och cybersäkerhet till angrepp. Denna ansats ger en heltäckande bild över vad som påverkar myndigheters, och i förlängningen samhällets informations- och cybersäkerhet. Detta innebär att de förebyggande åtgärder som vi rekommenderar tar sikte på samtliga delar av informationshanteringen oavsett hot. Detta i kombination med de insatser som görs av andra myndigheter med uppgifter inom informations- och cybersäkerhet, som exempelvis Försvarets Radioanstalt (FRA), Säkerhetspolisen och Försvarsmakten, borgar för att svenska myndigheter har tillgång till information och stöd för att bedriva sin verksamhet med ändamålsenlig informations- och cybersäkerhet.

Att upprätthålla informations- och cybersäkerhet är prioriterade även under situationer av kris eller i ett läge av höjd beredskap. I och med den återupptagna planeringen för totalförsvaret har MSB påbörjat arbetet med att se över och utveckla de delar av myndigheten och dess ansvarsområden som behöver fungera vid ett läge av höjd beredskap. Förmåga inom informations- och cybersäkerhet bedöms vara viktig att upprätthålla. Inom MSB:s ansvarsområde: samhällets informations- och cybersäkerhet ryms bland annat uppgiften att på förekommen anledning rapportera till regeringen om förhållanden rörande informations- och cybersäkerheten i samhället som kan leda till behov av att vidta åtgärder. För denna typ av rapportering är incidentrapporteringen från statliga myndigheter en, av flera, viktiga informationskällor.

MSB ska årligen presentera en sammanställning och analys av de rapporter om allvarliga it-incidenter som inkommit under det föregående kalenderåret[3,4].

2.1 När något går fel

Alla verksamheter kommer förr eller senare att drabbas av någon form av allvarlig it-incident. När detta sker har rapporteringspliktiga[5] myndigheter

3. I enlighet med kravet på årlig rapport i 11 a § 2 st förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

4. Inför sammanställningen av rapporten ska MSB enligt sin instruktion även inhämta upplysningar från Säkerhetspolisen och Försvarsmakten om de incidenter som rapporterats in till dessa myndigheter enligt 2 kap. 10 § första stycket 2 i säkerhetsskyddsförordningen (2018:658). Resultatet av denna inhämtning redovisas i bilaga 2 (sekretessbelagd).

5. Enligt 20 § i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, krisberedskapsförordningen, gäller rapporteringsskyldigheten för it-incidenter alla statliga myndigheter under regeringen, med undantag för Regeringskansliet, kommittéväsendet, Säkerhetspolisen, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut enligt 3 § i samma förordning. För utlandsmyndigheterna tillämpas bestämmelserna endast i den utsträckning som bestäms i föreskrifter som meddelas av Regeringskansliet (Utrikesdepartementet).

krav på att anmäla dessa till MSB[6]. Rapporterna mottas vid MSB av funktionen CERT-SE som bland annat bidrar med operativt stöd. Ibland kan det dock vara svårt att avgöra vad som är en rapporteringspliktig incident och därför behöver man inte ha konstaterat en incident för att vända sig till CERT-SE. Rapporterna som inkommer omfattas till största del av sekretess.[7] MSB:s arbete syftar främst till att ge stöd till myndigheterna att förebygga it-incidenter, i andra hand att stödja i hanteringen när de inträffar. MSB ger stöd till alla aktörer som vänder sig till CERT-SE, inte bara myndigheter. Stödet kan utgå från en rapporterad incident och en incident där stöd lämnats kan även generera en rapport.
De flesta it-incidentrapporter som inkommit är dock av den karaktären att inget stöd behövs, antingen för att myndigheten hanterat incidenten på egen hand eller för att rapporten lämnas så långt efter att händelsen inträffat att det inte är relevant att ge stöd.

2.1.1 Vilka ska rapportera?

I mars 2019 uppgick antalet rapporteringsskyldiga myndigheter till 251 stycken, vilket är en minskning med fem myndigheter sedan föregående år. Antalet myndigheter varierar från år till år då vissa tillkommer och andra faller ifrån. Det är vidare så att flera myndigheter i praktiken härbärgeras och driftas av andra myndigheter. Denna utveckling har skapat viss osäkerhet hos aktörerna gällande it-incidentrapporteringen. I vissa fall är systemen och informationen så sammanlänkad att det är svårt att avgöra vem som bör rapportera eventuella incidenter. Ett fåtal större myndigheter har aktivt tagit en roll att ansvara för mindre myndigheters it. Detta är i grund och botten en positiv utveckling, men det måste finnas en tydlighet gällande vems information som påverkas av eventuella it-incidenter så att de berörda parterna kan rapportera och agera på de incidenter som uppstår.

2.1.2 Vad som ska rapporteras

Statliga myndigheter ska ha rutiner för att identifiera, bedöma, rapportera, hantera och dokumentera incidenter som kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation.[8] Myndigheterna ska skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som *allvarligt* kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Det är upp till myndigheterna själva att bedöma vilka incidenter som är tillräckligt allvarliga för att omfattas av rapporteringsskyldigheten.

6. Alla statliga myndigheter ska enligt 20 § i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Rapporteringen ska ske till MSB, i enlighet med MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2). Rapporteringsskyldigheten omfattar inte sådana incidenter som ska rapporteras enligt 10 2. § i säkerhetsskyddsförordningen (2018:658).

7. Med stöd av 18 kap 8 § 3 p. i offentlighets och sekretesslagen (2009:400). Tillämpningen har prövats flera gånger i Kammarrätten, där domsluten stöder MSB:s ställningstagande till sekretessbedömningen. Se bland annat dom från Kammarrätten i Göteborg, mål nr 5032-16.

8. 10 § i MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1).

Rapporteringen av allvarliga it-incidenter till MSB ska innehålla uppgifter om bland annat tidpunkter för upptäckt, när incidenten inträffade och om den är pågående eller avslutad. Myndigheterna ska också uppge eventuell sekretess för uppgifterna i rapporten samt om händelsen är polisanmäld.[9] Rapporteringsförfarandet ses över under 2020 för att underlätta för de rapporterande myndigheterna, samt för att säkerställa att den information som MSB behöver för att kunna stödja operativt vid behov finns och för att dra rätt slutsatser om vilka åtgärder som krävs och vilka förebyggande insatser som har bäst effekt.

2.2 Övrig incidentrapportering

MSB är ansvarig myndighet gällande NIS-lagstiftningen och förordningen[10], vilket bland annat innebär att myndigheten tar emot incidentrapporter från verksamheter som berörs av regleringen samt utgör Sveriges CSIRT (Computer Security Incident Response Team). Denna rapportering skiljer sig åt från den av krisberedskapsförordningen reglerade incidentrapportering som är i fokus för denna rapport, men då det ändock handlar om it-incidenter rapporterade till MSB nämns NIS-rapporteringen här[11].

Skillnaderna mellan rapporteringen enligt NIS-lagstiftningen och krisberedskapsförordningen är flera. NIS-lagstiftningen riktar sig till identifierade leverantörer av samhällsviktiga och digitala tjänster i privat och offentlig sektor[12]. Vidare avgränsas NIS till sju sektorer: bankverksamhet, finansmarknadsinfrastruktur, digital infrastruktur, leverans och distribution av dricksvatten, energi, transport samt hälso- och sjukvård. För att en incident ska rapporteras till MSB krävs att en störning av leveransen av den samhällsviktiga tjänsten uppstår, samt att denna störning har sitt ursprung i en incident i ett nätverk eller informationssystem. Kriterierna för att incidentrapportera enligt NIS är således högre än den rapportering som denna rapport fokuserar på, där *incidenter som allvarligt kan påverka säkerheten* ska rapporteras.

Sedan NIS incidentrapportering inleddes i mars 2019 har ett 50 tal rapporter kommit in, dessa rapporter sammanfattas och redovisas till EU-kommissionen och Regeringskansliet årligen i februari. Dessa incidenter, tillsammans med de incidenter som inkommer till MSB enligt krisberedskapsförordningen, är en delmängd av den information som MSB använder för att skapa en förståelse för förhållandena gällande informations- och cybersäkerhet för samhället i stort och svenska myndigheter specifikt.

2.3 Nyttogörande av it-incidentrapportering

MSB bedriver ett strategiskt analysarbete kopplat till de inkommande rapporterna om allvarliga it-incidenter. Det underlag som rapporterna genererar är ett av flera underlag som används för att inrikta arbetet med samhällets informations- och cybersäkerhet. Den strategiska analysen kopplar samman det operativa

9. MSB:s föreskrifter för obligatorisk it-incidentrapportering för statliga myndigheter (MSBFS 2016:2)
10. 2018:1175
11. För mer information om NIS, se [https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/]
12. För information om anmälan se MSB:s föreskrift MSBFS 2018:7

arbetet som utförs med det långsiktiga förebyggande arbete som bedrivs. Då MSB har ett särskilt ansvarsområde med att stödja och samordna samhällets informations- och cybersäkerhet är det av stor vikt med en ändamålsenlig bild av hur läget ser ut bland statliga myndigheter.

Det är inte möjligt, eller önskvärt, att enbart det offentliga planerar och genomför insatser för att öka samhällets informations- och cybersäkerhet. Mycket av det som ska skyddas ligger utanför statens kontroll. Avregleringar och privatiseringar innebär att många samhällsviktiga verksamheter drivs av näringslivet. För att säkerställa att MSB når ut till det privata näringslivet med stöd genomför MSB insatser när det gäller privat-offentlig samverkan på informations- och cybersäkerhetsområdet.

2.4 Nya föreskrifter

Det är för få myndigheter som rapporterar it-incidenter och antalet rapporterade incidenter borde vara fler[13]. MSB reviderar därför föreskrifterna för incidentrapportering i syfte att det ska bli enklare för statliga myndigheter att avgöra vilka incidenter som ska rapporteras. De nya föreskrifterna ska också underlätta möjligheten att ge stöd vid den operativa hanteringen av en it-incident. I anslutning till att föreskrifterna träder i kraft kommer det tas fram en ny vägledning och ett nytt incidentrapporteringsformulär.

För att ytterligare inrikta och förbättra de statliga myndigheternas informations- och it-säkerhet reviderar och kompletterar MSB också föreskrifterna om informationssäkerhet för statliga myndigheter och utfärdar även nya föreskrifter om it-säkerhet för statliga myndigheter.

Den nya samt de reviderade föreskrifterna är:

Revidering av MSBFS 2016:1 ger ny föreskrift med nytt nummer – MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet

Revidering av MSBFS 2016:2 ger ny föreskrift med nytt nummer – MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter

Nya föreskrifter – MSB:s föreskrifter och allmänna råd om statliga myndigheters it-säkerhet.

De största förändringarna i föreskrifterna om informationssäkerhet består i att reglering om fysisk säkerhet och personalsäkerhet har lagts till. Dessutom har kraven på uppföljning och utvärdering konkretiserats ytterligare. De nya föreskrifterna om it-säkerhet för statliga myndigheter kompletterar föreskrifterna om informationssäkerhet genom att förtydliga hur skyddet för myndighetens it-miljö ska utformas. I föreskriften ställs exempelvis krav på att vidta utpekade säkerhetsåtgärder avseende riskbedömning, omvärldsbevakning, utveckling och anskaffning samt drift och förvaltning av informationssystem.

13. FOI redovisade i februari 2020 ett uppdrag till Justitiedepartementet där de undersökt orsaker till underrapportering av allvarliga it-incidenter till MSB, liksom av polisanmälningar då rapporterna rört angrepp. MSB gör en kort översikt över FOI:s resultat och slutsatser i kapitel 5, men hänvisar i övrigt till FOI:s rapport för statistiska underlag.

Exempel på operativt stöd

CERT-SE fick information från en forskare i ett annat land att det fanns sårbarheter i ett underliggande bibliotek i en samhällskritisk tjänst en myndighet levererar. Efter att CERT-SE varit i kontakt med myndighetens incidenthanterare inleddes interna undersökningar, där även myndighetens säkerhetsfunktion var delaktig. Säkerhetsansvarig undersökte den potentiella sårbarheten och försökte bekräfta informationen som CERT-SE hade delgett. Kontakt med övriga relevanta funktioner inom myndigheten hölls löpande under dagen. Ungefär tio timmar efter att informationen kom in var en ny version av tjänsten klar att läggas ut i produktion. All testning av tjänsten hade gått bra och beslut fattades att publicera den, vilket också skedde efter ytterligare några minuter.

Sårbarheten skulle ha kunna medfört en incident där känsliga personuppgifter spreds till obehöriga. Myndigheten bedömde dock risken att så faktiskt skett var låg, eftersom sannolikheten att någon skulle hittat luckan var liten. Efter incidenten reviderade myndigheten sina processer och införde rutiner för kontinuerlig uppdatering av stödtjänster och bibliotek för att på så vis avhjälpa risken för sårbarheter.

Rekommendation

Myndigheten har gjort allt rätt i detta fall, den agerade skyndsamt och åtgärdade den potentiellt kritiska incidenten. Förutom de processer som myndigheten själv sett över så är det viktigt att granska aktiviteten i samtliga loggar i it-miljön (systemloggar, trafikloggar etc.) om en sårbarhet upptäckts. Om det finns risk att inloggningsuppgifter så som användarnamn och lösenord har läckt, bör man också vidta åtgärder för att försäkra sig om att samma uppgifter inte använts även på andra tjänster.

It-incident-rapportering 2019

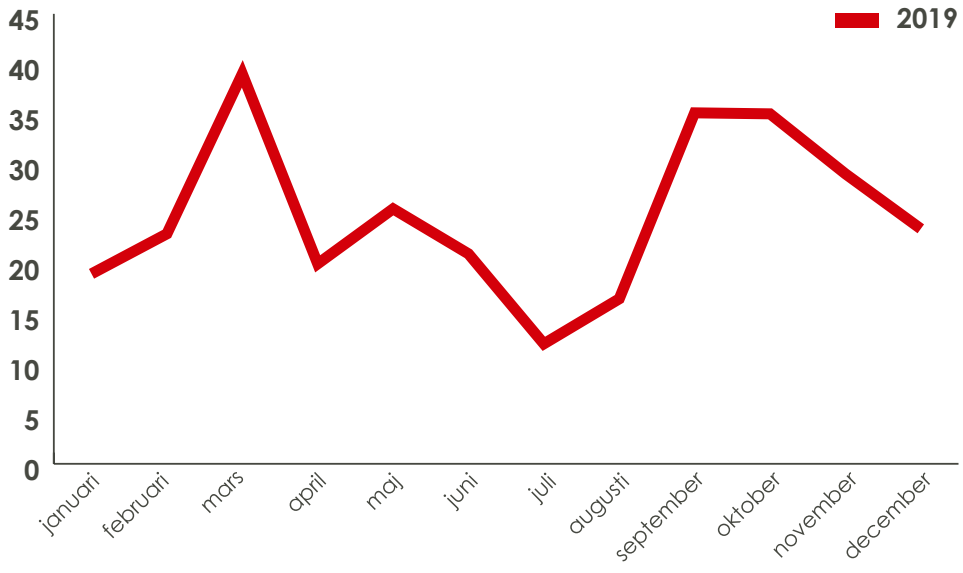
3. It-incidentrapportering 2019

I detta kapitel redovisas den it-incidentrapportering som MSB mottagit från statliga myndigheter under år 2019.

I enstaka fall har de rapporterande myndigheterna lämnat en preliminär rapport som sedan kompletterats. I de fallen har dessa endast räknats som en rapport. Däremot kan en och samma händelse generera it-incidentrapporter från flera myndigheter om flera myndigheter berörts, exempelvis vid elavbrott eller störningar i elektroniska kommunikationer.

Givet att myndigheterna själva avgör allvarlighetsgraden vid en incident, och därmed även om den är rapporteringspliktig, får MSB in rapporter om olika typer av incidenter. Det en myndighet bedömer som en rapporteringspliktig incident kan en annan myndighet bedöma som en mindre händelse som inte behöver rapporteras.

Rapporterna räknas utifrån det datum som de rapporterats till MSB, även om incidenten har upptäckts eller inträffat vid ett tidigare datum.



Figur 1. Linjediagram med antal inkomna it-incidentrapporter per månad 2019.

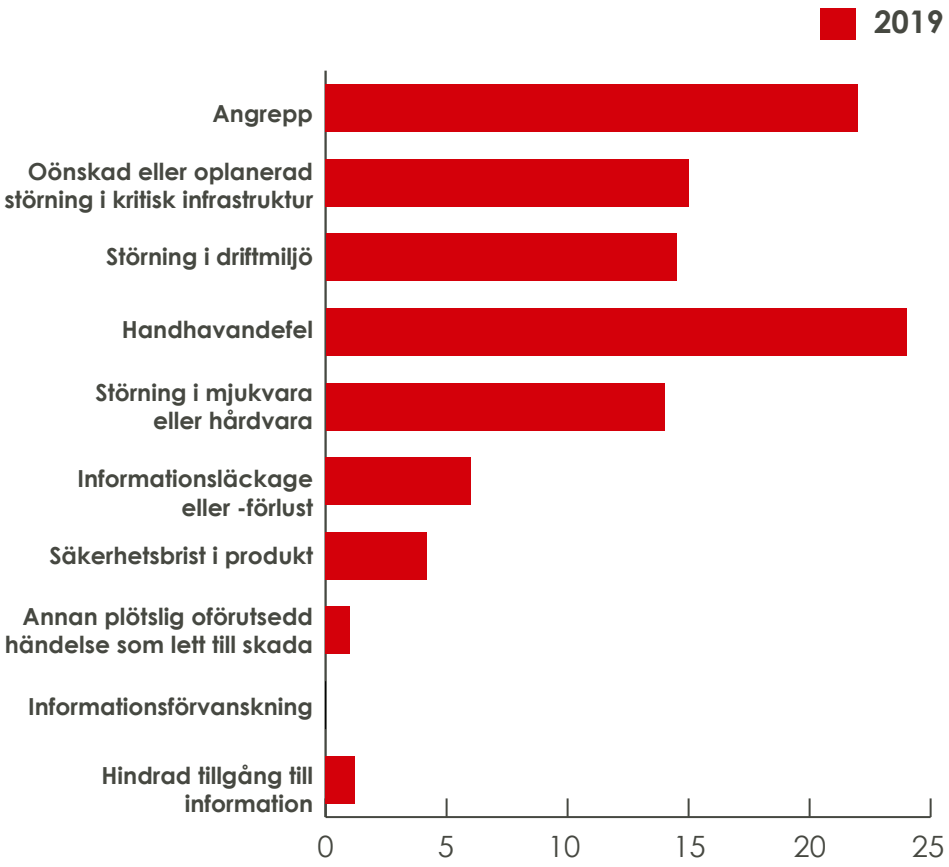
3.1 Antalet rapporter i stort oförändrat

Under 2019 inkom totalt 296 rapporter om allvarliga it-incidenter från de rapporteringsskyldiga myndigheterna.[14] Antalet myndigheter som lämnat minst en rapport under 2019 är 101 stycken och antalet myndigheter som inte lämnat någon rapport är 150 stycken, vilket ger en rapporteringsgrad på 40 %. Rapporternas fördelning över året visar på högre rapporteringsgrad under våren och hösten och en lägre nivå av rapporterade it-incidenter under sommaren och vintern.

3.2 Handhavandefel är den största kategorin

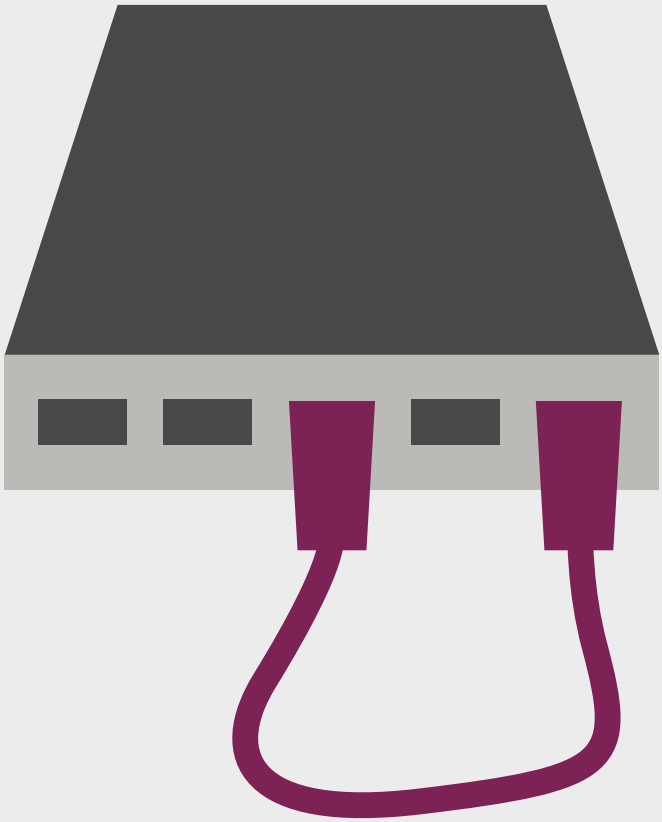
När en it-incident rapporteras går det att ange flera incidentkategorier för varje rapport. I de fall flera kategorier har angetts har rapporterade incidenter av MSB bedömts huvudsakligen tillhöra en incidentkategori.

De fyra största kategorierna för typ av it-incident under 2019 är i fallande ordning *handhavandefel* (68 rapporter), *angrepp* (62 rapporter), *oönskad eller oplanerad störning i kritisk infrastruktur* (45 rapporter) samt *störning i driftmiljö* (44 rapporter). Dessa fyra är tätt följd av kategorin *störning i mjukvara eller hårdvara* (41 rapporter) och tillsammans utgör dessa fem av tio kategorier 88 % av alla it-incidenter som rapporterats.



Figur 2. Stapeldiagram med procentuell fördelning av antal inkomna it-incidentrapporter per kategori 2019.

14. Rapporteringsgraden kan fortfarande vara påverkad av undantaget i rapporteringsskyldigheten i de fall en myndighet har utkontrakterat delar av sin it-drift innan föreskrifterna trädde i kraft. Detta i enlighet med 9 § i MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2).



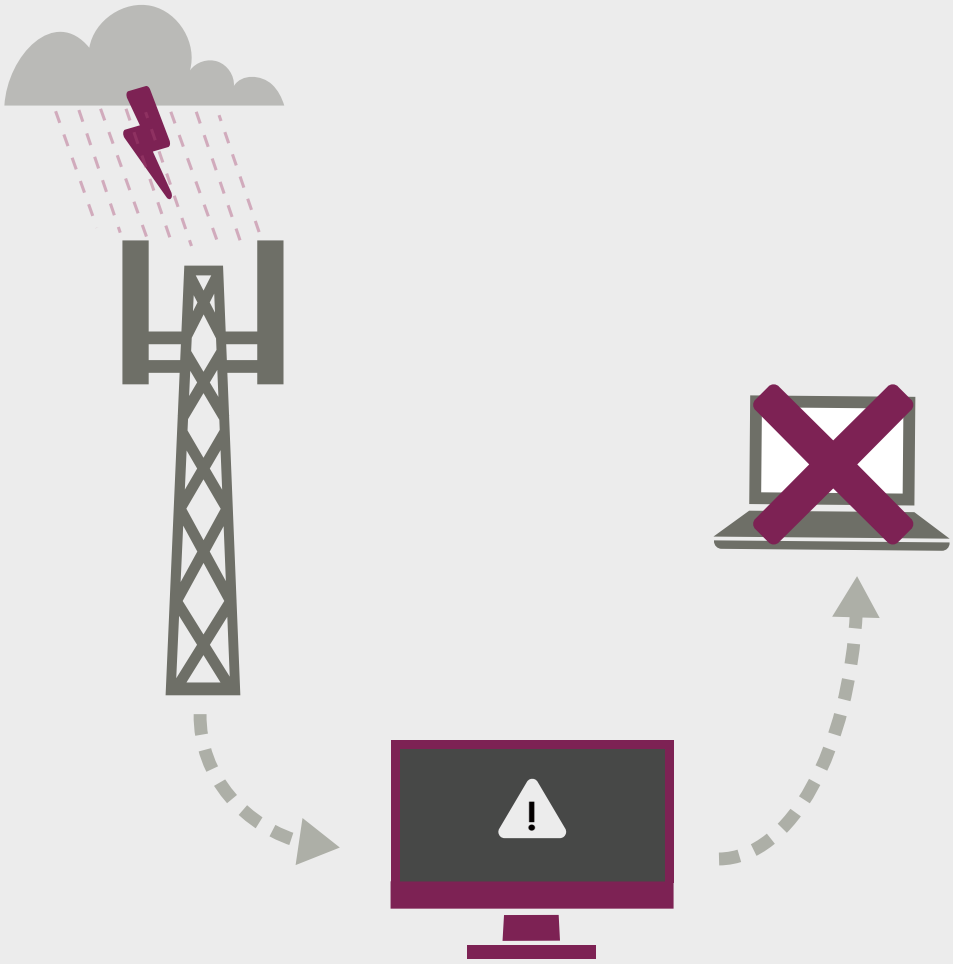
Exempel på handhavandefel

En anställd vid myndigheten skapade en nätverksloop via en switch, med totalstopp i nätverket som följd.

Initialt gjordes försök till felsökning genom att utföra omstarter av en central switch. När detta inte hjälpte upptäcktes väldigt många paketförluster på en specifik port. Efter ytterligare felsökningar kunde felet härledas till en specifik port på en lokal switch. Tekniker stängde av porten för vidare felsökning. I den aktuella porten satt en lokal omanagerad nätverksswitch som hade en nätverkskabel kopplad mellan två portar, vilket skapade en nätverksloop. Incidentens omfattning medförde att all nätverkstrafik på myndigheten påverkades. Vidare felsökning visade att det tilläggsprotokoll som skulle ha kunnat förhindra nätverksloopen (spanning tree) inte var korrekt konfigurerat. Detta hanterades av tekniker och implementerades överlag i myndighetens it-miljö.

Rekommendation

Det är enkelt att av misstag koppla ihop två portar och oavsiktligt skapa den här typen av problem. Det finns tekniska lösningar som kan upptäcka om så skett, exempelvis loopskydd som sänder protokollpaket från portarna där skyddet aktiverats. Om det upptäcker att protokollet tar emot samma paket i en port som sänder, stängs porten som protokollet skickades från ned. Se även till att endast behörig personal kan göra förändringar i nätverk, nätverksstruktur- och topologi.



Exempel på störning i driftmiljö

Ett blixtnedslag slog ut en dator, vilket innebar allvarliga störningar i en myndighets samhällskritiska verksamhet, i nästan ett dygn. Ingen reservdator av den typ som behövs för verksamheten fanns på plats utan en tekniker var tvungen att ta med sig en dator från annan ort och konfigurera den.

På grund av bristande rutiner förvärrades konsekvenserna av incidenten. Enligt dokumentation skulle en färdigkonfigurerad reservdator finnas på plats, men på grund av bristande rutiner var så inte fallet.

Incidenten fick stora konsekvenser på leverans av samhällskritisk tjänst.

Rekommendation

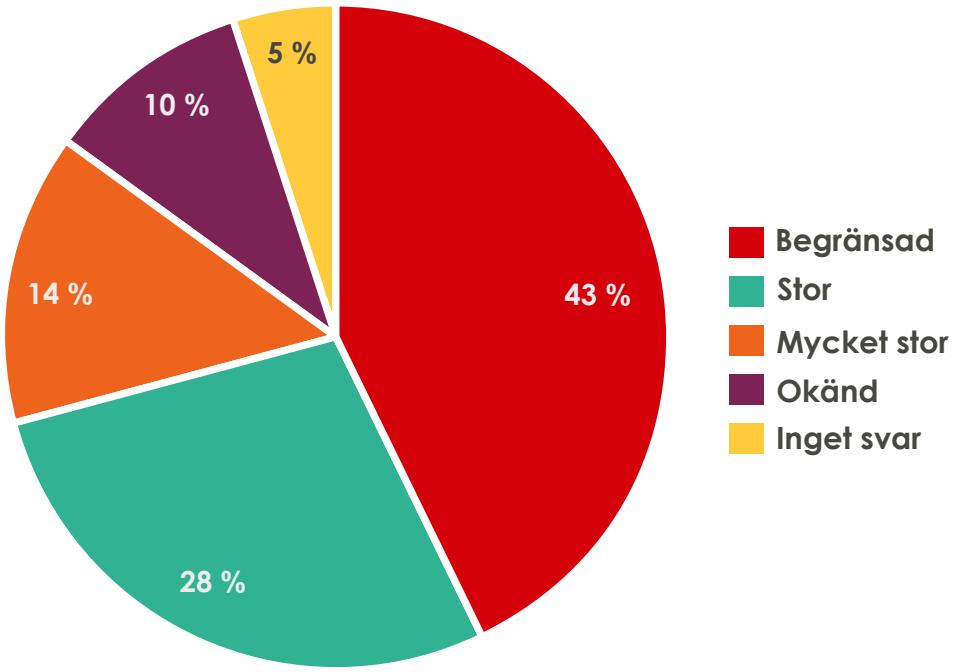
Vädret är svårt att rå på men interna rutiner kan man däremot ha bättre kontroll över. När det gäller samhällskritisk verksamhet är det av yttersta vikt att ha reservutrustning nära till hands, och redo för användning, för att minimera samhällsstörningen i tid och omfång. Rutinerna och dokumentationen kring detta bör ses över så att liknande händelser inte inträffar.

3.3 Konsekvenser

Konsekvensen för den rapporterade it-incidenten bedöms av den rapporterande myndigheten.

Den mest frekventa konsekvenskategorin är begränsad konsekvens (126 rapporter) vilket svarar för 43 % av alla anmälda it-incidenter. Stor konsekvens är den näst vanligaste (84 rapporter) följt av mycket stor konsekvens (41 rapporter) och okänd konsekvens (30 rapporter). I 15 rapporter angavs ingen konsekvens.

De kategorier som är vanligast förekommande bland incidenter som fått stora eller mycket stora konsekvenser är oönskad eller oplanerad störning i kritisk infrastruktur, störning i driftmiljö samt handhavandefel. För kategorin angrepp är det få incidenter som av myndigheterna anges ha fått annat än begränsade konsekvenser.



Figur 3. Cirkeldiagram med procentuell fördelning av it-incidentrapporter per konsekvenskategori 2019.

It-incident-rapportering 2016–2019

4. It-incidentrapportering 2016–2019

I detta kapitel redovisas den rapportering som skett under 2016–2019 för att sätta rapporteringen i föregående kapitel i en kontext samt som ett inledande material inför analys i kommande kapitel, men också som en summering över perioden.

I enstaka fall har myndigheterna lämnat en preliminär rapport som sedan kompletterats. I de fallen har detta endast räknats som en rapport. Däremot kan en och samma händelse generera it-incidentrapporter från flera myndigheter om flera myndigheter berörts, exempelvis vid elavbrott eller störningar i elektroniska kommunikationer.

Givet att myndigheterna själva avgör allvarlighetsgraden vid en incident, och därmed även om den är rapporteringspliktig, får MSB in rapporter om olika typer av incidenter. Det en myndighet bedömer som en rapporteringspliktig incident kan en annan myndighet bedöma som en mindre händelse som inte behöver rapporteras.

Rapporterna räknas utifrån det datum som de rapporterats till MSB, även om incidenten har upptäckts eller inträffat vid ett tidigare datum.

4.1 Fler myndigheter rapporterar

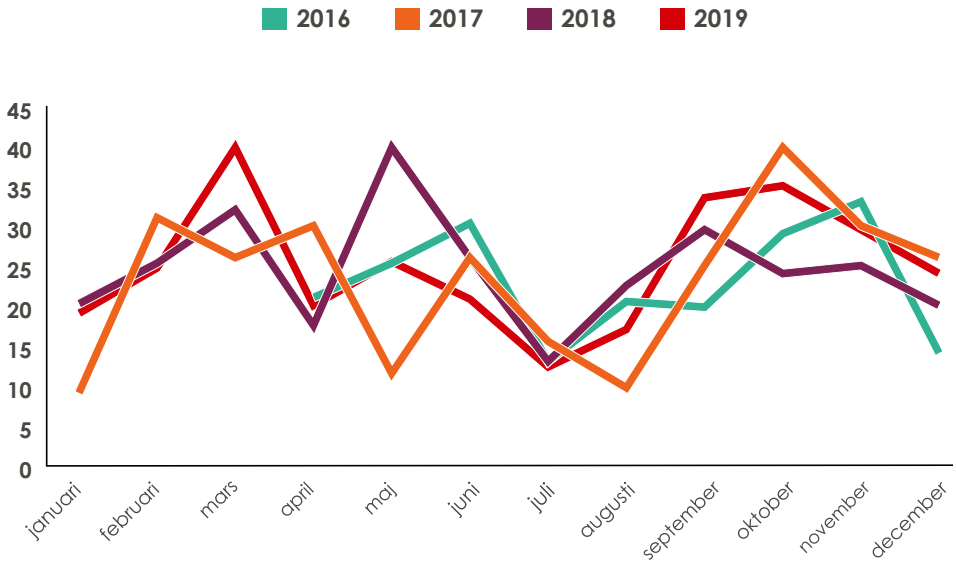
Under de två senaste åren har antalet rapporteringspliktiga myndigheter varit något högre än under de två första åren. Ökningen av antalet rapporterade incidenter som skedde under de tre första åren har avstannat, dock har andelen myndigheter som rapporterat in incidenter ökat. Flera myndigheter har lämnat en eller flera rapporter under vissa år, men inga alls under andra år.

Tabell 1. Antal rapporteringspliktiga myndigheter, antal rapporterande myndigheter och antalet lämnade rapporter för 2016–2019

	2016	2017	2018	2019
Antal rapporteringspliktiga myndigheter	244	244	256	251
Antal (andel) rapporterande myndigheter	77 (32 %)	79 (32 %)	87 (34 %)	101 (40 %)
Antal inlämnade it-incidentrapporter	214 (285)[15]	281	297	296

Rapporteringsgraden varierar över året, men har sedan starten i april 2016 inte förändrats i någon större omfattning.

15. Då incidentrapporteringen startade först i april 2016 har det redovisade antalet it-incidentrapporter även justerats för brutet räkenskapsår.



Figur 4. Linjediagram med antal inkomna it-incidentrapporter per månad 2016–2019

4.2 Handhavandefel har ökat

Vid rapportering av en allvarlig it-incident går det att ange flera incidentkategorier för varje rapport. Exempelvis kan en it-incident i driftmiljön orsakas av ett angrepp som leder till hindrad tillgång till information och således kan rapporterande myndighet välja att ange två kategorier. Rapporterade incidenter har av MSB bedömts huvudsakligen tillhöra en incidentkategori. Enligt denna bedömning har rapporterna varit fördelade enligt nedanstående tabell.

Tabell 2. Rapporterade allvarliga it-incidenter per kategori 2016-2019.

Kategori	Antal 2016	Antal 2017	Antal 2018	Antal 2019
Angrepp	66	78	73	62
Oönskad eller oplanerad störning i kritisk infrastruktur	9	18	59	45
Störning i driftmiljö	66	45	47	44
Handhavandefel	17	50	42	68
Störning i mjukvara eller hårdvara	38	60	38	41
Informationsläckage eller -förlust	11	3	21	19
Säkerhetsbrist i produkt	2	12	14	13
Annan plötslig oförutsedd händelse som lett till skada	0	9	3	2
Informationsförvanskning	0	4	0	0
Hindrad tillgång till information	5	2	0	2
Totalt	**214**	**281**	**297**	**296**

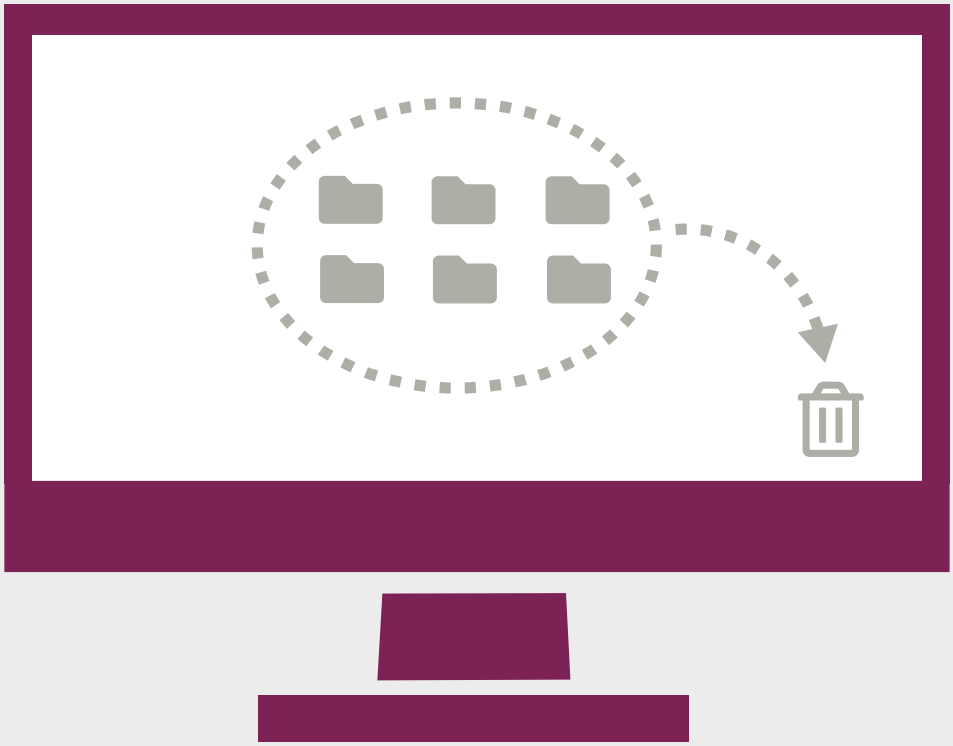
Exempel på handhavandefel

Vid en kontroll av myndighetens ftp-konton (file transfer protocol), som del av ett arbete med att avveckla dessa, konstaterades att ett konto hade satts upp på sådant vis att en fil låg tillgänglig för alla som hade åtkomst till kontot. Lösningen hade varit uppsatt på detta sätt sedan flera år tillbaka. De som hade åtkomst till kontot var organisationer som rapporterar in känsliga uppgifter, bland annat om sina anställda. Flera fel hade begåtts i fallet, bland annat hade interna krav på behörighetsstyrning inte efterlevts då flera organisationer hade tillgång till samma ftp-konto. Vidare hade uppgifter kunnat lämnas via en okrypterad förbindelse. Det fanns också en risk att enskilda filer potentiellt funnits tillgängliga för andra organisationer då de hade tillgång till samma konto.

De flesta organisationer som rapporterar in uppgifter har maskin-till-maskin-överlämnande av filer men de som hade tillgång till kontot hade således möjligheten att logga in manuellt. Därför fanns risken att olika organisationer kunde se varandras information som längst en timme för varje lämnad fil, innan den flyttades. Det fanns även en risk att någon med tillgång till kontot skulle ha kunnat ladda ner information på regelbunden basis. Den kortsiktiga lösningen på problemet var att stänga kontot helt och säkerställa att uppgiftslämnare använde det säkrare protokollet sftp (secure file transfer protocol), som garanterar bättre behörighetshantering och krypterad överföring.

Rekommendation

Det är olämpligt att flera olika användare har tillgång till samma ftp-konto för överföring och hantering av filer, särskilt sådana med känsligt innehåll. Om flera använder samma konto försvåras möjligheten att spåra vem som gjort vad, och vem som tagit del av informationen som är publicerad där. Dessutom saknar ftp-protokollet tillräckliga krypteringsfunktioner för hantering av känsliga person-uppgifter. Istället bör det säkrare alternativet sftp användas, och i fallet ovan fanns detta de facto tillgängligt att använda. Det bör också införa metoder för verifiering av sin it-miljö, så att det finns en person som är ytterst ansvarig för att säkerställa att kravspecifikationen för den levererade tjänsten uppfylls.



Exempel på informationsläckage eller -förlust

En händelse av informationsförlust inträffade på en myndighet då en anställd hade skickat in en begäran om att tre lagringsytor skulle tas bort, vilket en tekniker utförde. Den anställde var dock inte medveten om att både backup- och arkivdata ingick i samma lagringsyta. Två månader efter verkställandet återkom den anställde och ville läsa arkivdata från dessa lagringsytor, vilket inte var möjligt då all information som var sparad i dessa ytor var raderad. Myndigheten hade fått information om att det bara var backupdata som skulle försvinna om man raderade en lagringsyta, men så var inte fallet. Det har alltid varit så att både backup- och arkivdata tas bort vid radering.

Konsekvensen av denna incident var att relevant data gick förlorad då den inte gick att återställa efter så pass lång tid.

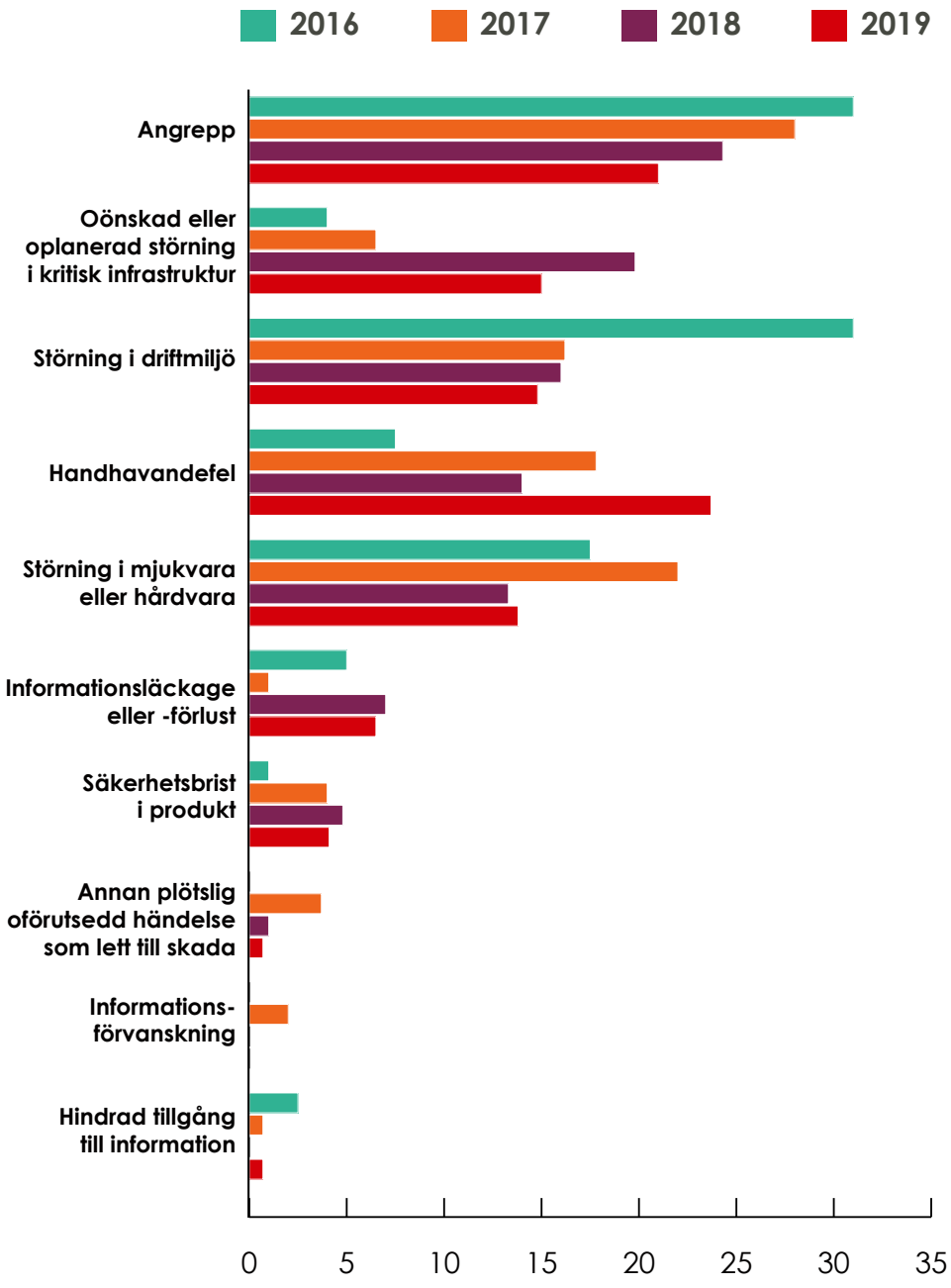
Rekommendation

Man bör se till att inte ha sin backup och sitt arkiv på samma ställe. Gör skillnad på produktionsdata (det vill säga levande dokument som används under arbetets gång) och den information som ska lagras under en längre tid eller permanent. Det är också lämpligt att ha en extra backup på annan fysisk plats. Om den enda backupen ligger aktivt i nätet finns risken att den krypteras vid en eventuell ransomware-attack.

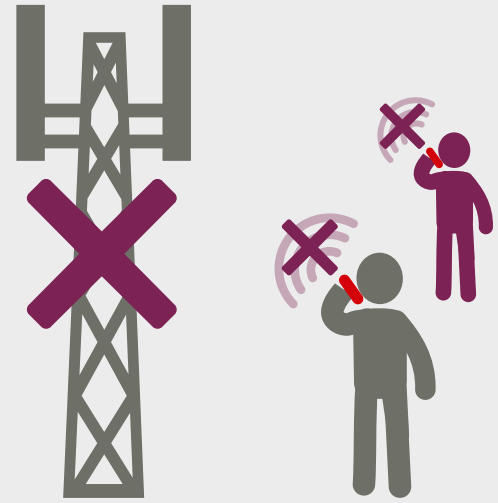
När man gör en förändring i it-miljön bör man även se över sina verifieringsrutiner, så att de genomförda ändringarna överensstämmer med de uppställda förväntningarna. Om det finns avvikelser så är sannolikheten att kunna återställa informationen större ju närmre händelsen i tid man är, så det är viktigt att dessa upptäcks skyndsamt.

Handhavandefel och angrepp utgör de största incidentkategorierna med ungefär en femtedel vardera av de rapporterade it-incidenterna. Därefter följer oönskad eller oplanerad störning i kritisk infrastruktur samt störning i driftmiljö och störning i mjukvara eller hårdvara.

Andelen rapporterade angrepp har gått stadigt nedåt under de senaste fyra åren, medan det har skett en ökning av handhavandefel och störningar i kritisk infrastruktur.



Figur 5. Andelen rapporterade it-incidenter indelat efter kategori åren 2016–2019.



Exempel på oönskad eller oplanerad störning i kritisk infrastruktur

En eftermiddag drabbades myndigheten av ett avbrott hos sin mobiltelefoni-operatör. Myndighetens möjligheter att kommunicera med omvärlden med mobiltelefon blev då mycket begränsade. Samtal tappades, bröts, var helt tysta eller gick inte fram. Detta medförde stor påverkan på flera verksamhetsområden inom myndigheten, med effekter för såväl anställda som allmänheten.

Samma kväll klarskrevs incidenten av mobiloperatören men problemen återkom efterföljande morgon, och pågick då fram till eftermiddagen. Incidenten klarskrevs igen på eftermiddagen dag två, med undantag för kapacitetsproblem till och från mobiloperatören. Detta medförde i sin tur problem med övervakningslösningar som gick på mobiloperatörens nät. Detta problem åtgärdades under kvällen dag två. Följande dag genomförde mobiloperatören åtgärdsarbeten och uppgraderade då utrustning.

Totalt drabbades myndigheten under en och en halv dag. Under denna tidsperiod kompletterades mobiltelefonitjänsten med fasta telefoner samt mobiltelefoner med annan operatör.

Rekommendation

För verksamheter som levererar samhällskritiska tjänster är det viktigt att upphandla redundanta leverantörer, så att man snabbt kan ställa om till en annan aktör om problem med tjänsteleverans eller liknande uppstår.

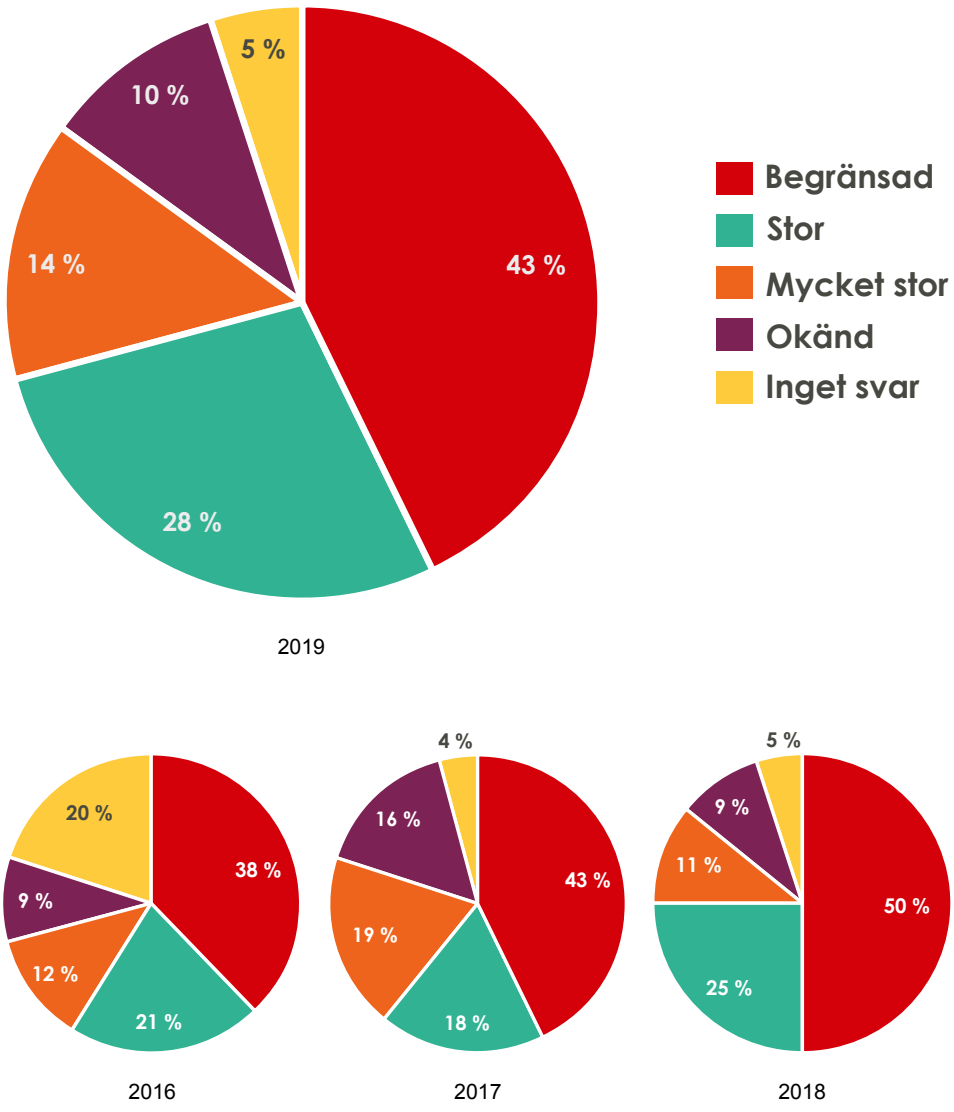
Myndigheter med anslutning till SGSI (Swedish Government Secure Intranet), ett nätverk för datakommunikation mellan myndigheter som är skilt från internet, har generellt bättre redundans och klarar därmed störningar bättre. För ytterligare redundans gällande telefoni bör myndigheter se över möjligheten till användandet av Rakel[1].

Det är även viktigt att upphandla tydliga serviceavtal om vilka krav som ställs på tjänsten. Förutom krav på kostnader, driftsäkerhet, antal fel och hastighet bör incidenthantering vara ett krav. Kraven bör anges så att de blir mätbara.

1. Rakel är ett digitalt radiokommunikationssystem för trygg och säker kommunikation mellan medarbetare inom samhällsviktig verksamhet, för mer information se msb.se/rakel

4.3 Konsekvenser

Omfattningen av konsekvenserna bedöms av den rapporteringsskyldiga myndigheten. För 2018 och 2019 har cirka tre fjärdedelar av konsekvenserna varit begränsade eller stora, medan motsvarande andel för 2016 och 2017 var två tredjedelar. Andelen allvarliga it-incidenter där konsekvenserna varit mycket stora, okända eller inte har angetts verkar ha stabiliserats de senaste två åren, där andelen mycket stora konsekvenser ligger strax över 10 %. Den enda kategori som följt en tydlig utveckling över samtliga fyra åren är konsekvens-kategorin stor, som ökat för varje år.



Figur 6. Fördelning av omfattning av konsekvenser för rapporterade it-incidenter under 2019 samt 2016–2018.

4.4 Angrepp och polisanmälan

Vid angrepp, eller vid misstanke om att it-incidenten har sitt ursprung i en brottslig gärning, uppmanar MSB den rapporterande myndigheten att göra en polisanmälan. I det arbete som sker med att uppdatera frågeformuläret för att rapportera allvarliga it-incidenter kommer frågan om incidenten misstänks ha sitt ursprung i en brottslig gärning ställas tidigt, och i de fall där det är tillämpbart uppmanas myndigheterna att polisanmäla incidenten. I en internationell jämförelse förefaller det vara så att de flesta nationer använder den modell som används i Sverige, det vill säga att varje enskild myndighet ansvarar för att göra bedömningen och där det är tillämpbart polisanmäla. För att säkerställa att de incidenter som har sin grund i brottslig gärning anmäls till Polismyndigheten har MSB och Polismyndigheten fördjupat informationsdelningen. Dessutom är båda myndigheterna är en del av det kommande nationella cybersäkerhetscentret.

I kategori *angrepp* ingår cyberangrepp, exempelvis dataintrång, bedrägeri och överbelastningsattacker. Fysiska tillgrepp som inbrott och stöld där exempelvis datorer eller mobiltelefoner förlorats, rapporteras oftast i kategorin *informationsförlust*. Därav finns det polisanmälda allvarliga it-incidenter som inte ingår i kategorin *angrepp*.

Tabell 3. Andelen polisanmälda it-incidenter 2016–2019.

	2016	2017	2018	2019
Andel angrepp (av antalet rapporter)	31 %	28 %	25 %	21 %
Andel polisanmälda angrepp (av antalet angrepp)	18 %	12 %	11 %	21 %
Andel polisanmälda incidenter (av totala antalet rapporter oavsett kategori)	6 %	5 %	7 %	6 %

Andelen angrepp som polisanmälts har stigit under 2019, men fortfarande anmäls cirka en femtedel av de angrepp som rapporteras till MSB. Av dessa angrepp utgörs en stor andel av phishingförsök, där endast ett fåtal lyckats. Den totala andelen polisanmälda incidenter har sedan 2016 legat på en konstant nivå.

Beroende på vilken typ av informationssystem som angripits ska anmälan om misstänkt brott göras antingen till Polismyndigheten eller till Säkerhetspolisen. I det fall Försvarsmakten är tillsynsmyndighet ska rapporteringen även gå till dem.[16] Sådana anmälningar behandlas i bilaga 2 (sekretessbelagd).

16. Fram till 31 mars 2019 enligt 1996:663. Från 1 april 2019 gäller ny säkerhetsskyddslagstiftning med något ändrade formuleringar kring vad som omfattas av rapporteringsskyldigheten utifrån 2 kap 10 § i säkerhetsskyddsförordningen (2018:658).

Exempel på angrepp

En användare i ett hr-system på en myndighet upptäckte att denne hade tillgång till information som personen inte skulle ha tillgång till, och hade på så sätt kunnat hämta ut ytterligare uppgifter för vilka behörighet saknats. Informationen tillgängliggjordes genom en sql-injektion (structured query language). Användaren uppmärksammade detta för sin chef, och blev påtalad det olämpliga i att utnyttja detta. Ytterligare slagningar skedde och därför beslutade myndigheten att polisanmäla incidenten. Funktionaliteten som möjliggjorde ett utnyttjande stängdes av då buggen blev känd, och rättades i en ny version av hr-systemet några dagar senare.

Rekommendation

Generellt bör man uppdatera sårbarheter i produkter så snart som det är möjligt. När det gäller att förhindra sql-injektioner är den första åtgärden att kontrollera vilka applikationer (om några alls) är sårbara. Ett sätt är att utföra penetrationstester på applikationerna i sin it-miljö, för att se om det går att komma åt de egna systemen eller information i dem. Tänk på att applikationer bör utvecklas i enighet med erkända ramverk och genomgå tester baserade på exempelvis OWASP[17] och PTES[18]. Indatavalidering ska användas för att skydda applikationen eller tjänsten mot att felaktig data används och kan orsaka fel.

När det gäller att åtgärda sårbarheter för sql-attacker kommer man även långt med så kallade prepared statements, en funktion som används för att utföra samma eller liknande databasuppdrag upprepade gånger med hög effektivitet. Vid sql-injektioner används ofta en förberedd mall där vissa konstanta värden ersätts under varje exekvering.

17. Open web application security project
18. Penetration testing execution standard

Analys av it-incident-rapporteringen

5. Analys av it-incident-rapporteringen

Detta kapitel innehåller analys av de inkomna rapporterna om allvarliga it-incidenter, vilket ligger till grund för följande kapitel om stöd och rekommendationer till både de myndigheter som träffas av MSB:s föreskrifter, men även till övriga aktörer. Sammanfattningsvis ser MSB med oro på den kombinerade utvecklingen av ökande andel handhavandefel, föråldrade it-miljöer hos svenska myndigheter och intensifierad digitalisering. I en komplex och i vissa fall föråldrad it-miljö kan enskilda handhavandefel få stora, och ibland svårligen upptäckta och korrigerbara följder. Denna problematik är oroande och det krävs krafttag för att både modernisera och göra it-system transparenta, spårbara och säkra. Samtidigt som de som arbetar i systemen måste kompetensutvecklas, både för att möta den nya tekniken, men också för att kunna ansvara och ta hand om den transformation av samhällets informationshantering som sker. Ytterligare försvårande omständigheter är det faktum att den höga andelen handhavandefel kan indikera en generell kompetensbrist. Givet den generella kompetensbristen kan det antas att kompetensen om att det ska, och vad, som ska rapporteras också är eftersatt.

MSB bedömer att det föreligger en risk att kommande års it-incidenter kommer att få allt allvarligare konsekvenser i takt med att digitaliseringen av myndigheternas informationshantering fortsätter. För att motverka denna utveckling behöver arbetet med information- och cybersäkerhet prioriteras, resurssättas och utvecklas hos statliga myndigheter de kommande åren.

5.1 Fler kan rapportera mer

MSB har sedan den första årsrapporten publicerades våren 2017 konstaterat samma sak varje år: det är för få incidenter som rapporteras, och för få myndigheter som rapporterar, även om antalet rapporterande myndigheter har ökat. Orsaken till frånvaron av rapportering kan variera, och FOI har haft ett särskilt uppdrag från regeringen att ytterligare belysa detta. Rapporten[19] visar att anledningarna till varför en myndighet valt att inte rapportera är flera och varierande. Några exempel på detta är att rutiner för att identifiera, bedöma, hantera, dokumentera och rapportera it-incidenter saknas eller är bristfälliga, hög arbetsbelastning på myndigheten, bristande rutiner för att hantera överföring av sekretessbelagd information, svårigheter i att bedöma it-incidenters allvarlighetsgrad samt att myndigheten inte upplever någon nytta med rapporteringen. Flera anledningar som nämns i rapporten är att befintliga rutiner inte är inarbetade, bristande intern informationsdelning, svårigheter rörande bedömning och hantering av

19. IT-incidenter på statliga myndigheter. Orsaker till utebliven rapportering, Rapportnummer: FOI-R--4815--SE

sekretessbelagd information, samt otillräcklig återkoppling från MSB. Rapporten problematiserar vidare myndigheternas upplevda oklarhet gällande rapporteringsskyldighet samt ansvarsfördelning när värdmyndigheter för it-drift används.

Arbetet med att revidera föreskrifterna som reglerar incidentrapporteringen har inkluderat underrapporteringsproblematiken som en, av många, ingångsvariabler. Huruvida uppdaterade föreskrifter kommer att underlätta för myndigheterna att avgöra när, vad och varför de ska rapportera in it-incidenter får utvärderas när de trätt i kraft, och varit gällande under en tid. Då myndigheter skiljer sig åt på alla plan sett till uppdrag, storlek, placeringsort med mera är det svårt att dra generella slutsatser varför de inte rapporterar i den utsträckning som MSB förväntar sig. För att bättre förstå, samt initiera kontakt, har vi under 2019 påbörjat ett projekt med att kontakta samtliga myndigheter för att undersöka huruvida något specifikt stöd behövs gällande informations- och cybersäkerhet. Denna kontakt har, baserat på det ökande antalet myndigheter som rapporterar, inneburit att flera myndigheter integrerat MSB i sin incidenthanteringsprocess, och därmed rapporterat incidenter som bedöms som allvarliga. MSB har identifierat ett behov av att öka synligheten för att kunna marknadsföra och tillgängliggöra det stöd som erbjuds, och den resurs MSB är för myndigheter när det gäller informations- och cybersäkerhet.

Ytterligare en faktor som påverkar den upplevt låga rapporteringsgraden är de myndigheter som har i stort sett hela sin it-drift och -miljö hos en annan myndighet. Det har visat sig vara otydligt för de aktuella myndigheterna i dessa fall vem som ska rapportera, vilket i vissa fall har lett till att ingen rapport kommit till MSB. Rapporteringsplikten gäller statliga myndigheter under Regeringskansliet, denna grupp består av många olika myndigheter, vissa med tydliga kopplingar till andra myndigheter i frågan om informationshantering. I de fall när en större myndighet huserar en annan myndighets it-drift kan det vara svårt, givet de komplexa och i vissa fall, ålderstigna system som används att tydligt veta vems information som är drabbad, och i vilken utsträckning. Denna problematik förstärks av initiativ att dela och tillgängliggöra information mellan myndigheter för att underlätta hantering av ärenden, eller annan handläggning hos respektive myndighet. I vissa fall driftas myndigheterna av aktörer som inte är rapporteringspliktiga, vilket leder till oklarheter hur dessa överhuvudtaget ska rapportera incidenter till MSB. Detta gör att statistiken rörande hur stor andel av myndigheterna som rapporterar allvarliga it-incidenter till MSB behöver läsas med förståelsen att totalen inkluderar myndigheter som i praktiken inte kan rapportera incidenter till MSB.

5.2 Mycket går att förebygga

De flesta av de allvarliga it-incidenter som rapporteras till MSB, och särskilt de som får stora eller mycket stora konsekvenser, beror på mänskliga misstag och problem med tekniska lösningar.[20] Detta är också en trend som förstärkts under den tid som rapporteringsskyldigheten funnits. Samtidigt har de senaste årens attacker och it-incidenter visat på sårbarheterna i samhället när det förebyggande arbetet inte varit tillräckligt utvecklat. Dessa uppmärksammade fall har dock

20. Detta stämmer även överens med de incidenter som rapporteras till datainspektionen enligt GDPR där ungefär 60 % av incidenterna beror på mänskliga misstag, för mer information se https://www.datainspektionen.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2018.pdf

förstärkts av att de drabbade organisationerna inte har haft ett systematiskt och riskbaserat arbete fullt ut när det kommer till informations- och cybersäkerhet.

En ökad digitalisering, exempelvis genom ökad användning av molnlösningar och uppkopplade enheter (IoT), medför ett ökat beroende av kritisk infrastruktur, där störningar kan få stora konsekvenser för myndigheternas arbete, och därmed också medborgarnas förtroende för myndigheterna. Digitaliseringen medför ett kraftigt ökat behov hos myndigheterna att ha god ordning på sin information. Var finns den, vem har tillgång till den, vem ansvarar för den, och vilka behov finns gällande tillgänglighet, riktighet och konfidentialitet? Att informationsklassa och regelbundet analysera vilka hot, risker och sårbarheter relaterat till informationen som myndigheten hanterar är kritiskt för att i förlängningen behålla förtroendet för myndighetens verksamhet.

Riksrevisionen har uppmärksammat problematiken kring föråldrade it-system inom staten och de svårigheter de medför kring säkerhet och integrering med mer moderna system. Att behöva hantera system som när de byggdes inte hade samma säkerhetskrav är en sak, men att digitalisera idag utan att tänka säkert från början är oacceptabelt. Fler incidenter som rapporterats under det senaste året handlar om driftproblem och säkerhetsbrister i programvara som inneburit stora störningar i myndigheters verksamhet. När kraven på digitalisering och integrering av olika system ökar innebär det att förändringar behöver byggas genom security by design, det vill säga att tänka säkert från början. Detsamma gäller även när myndigheter utkontrakterar sin it-drift, antingen till andra myndigheter eller till privata aktörer genom upphandling.[21] Informationssäkerhetsansvaret kan aldrig utkontrakteras, den är myndighetens ledning alltid ytterst ansvarig för. Att hänvisa informationssäkerhet till it- eller säkerhetsansvariga är inte heller en lösning. Informationssäkerhet är något som angår hela myndigheten, precis som övrig verksamhetsstyrning.

Myndigheter behöver säkerställa att rätt kompetens gällande omvärldsbevakning och analys av ny teknologi finns tillgänglig. Myndigheters digitalisering förhåller sig till omvärlden och inte sällan förlitar de sig på utkontrakterade lösningar för att uppnå de aningen aggressivt satta digitaliseringsmål de förhåller sig till. Denna utveckling är vansklig och kan leda till stora sårbarheter och allvarliga konsekvenser för samhället. I och med den hastiga och ibland ogenomtänkta digitaliseringen som samhället genomgår, utan hänsyn till säkerheten i lösningarna, prioriteras eller glöms ibland säkerheten bort och kopplas på som ett sent påhäng i processen. Detta leder aldrig eller sällan till en ändamålsenlig säkerhet utan snarare en osäker digitalisering. Alternativt leder detta till en väldigt mycket dyrare process än vad som hade varit fallet om säkerhet hade inkluderats från början.

21. För vägledning gällande upphandling se: https://www.msb.se/sv/publikationer/upphandling-till-samhallsviktig-verksamhet--en-vagledning/
Samt: https://www.msb.se/sv/publikationer/upphandla-informationssakert--en-vagledning

Rekommenda-tioner

6. Rekommendationer

Den här rapporten har tydligt visat på behovet av ett utvecklat arbete med informations- och cybersäkerhet hos statliga myndigheter. MSB satsar för att kunna lämna bättre stöd till myndigheter och andra aktörer i samhället för att uppfylla regeringens ambitioner i cybersäkerhetsstrategin från 2018. I det ingår bland annat reviderade och nya föreskrifter på området, ett utökat metodstöd och utvecklad återkoppling och erfarenhetsåterföring gentemot myndigheter och näringslivet. Men detta kommer inte göra tillräcklig skillnad om inte övriga myndigheter också gör motsvarande ansträngningar.

6.1 Höj lägstanivån

Det är angeläget att med kraftfulla åtgärder fortsätta höja grundnivån av informations- och cybersäkerhet i samhället. Tack vare ökade medel för verksamheten, samt nya uppgifter och mandat, har MSB på senare år kunnat intensifiera sitt arbete med att höja informations- och cybersäkerhetsförmågan i samhället. När det gäller offentlig sektor sätter nu MSB med hjälp av nya föreskrifter för första gången en grundnivå för statliga myndigheters it-säkerhet och skärper dessutom kraven på myndigheternas systematiska informationssäkerhetsarbete. En skärpning av regleringen, teknisk utveckling och utökad uppföljning kommer innebära ett ökat behov av stöd och råd, vilket medför ökade förväntningar på MSB som aktör. MSB har på senare tid även fått ett flertal regeringsuppdrag om att tillhandahålla utbildningar i både privat och offentlig sektor.[22] Stödet till kommuner, regioner och statliga myndigheter kommer därmed att öka genom praktiska utbildningar och forum för samverkan. I detta ingår även att, vid behov, särskilt utveckla stöd till mindre myndigheter.

Med stöd av NIS-regleringen ställer MSB nu enhetliga krav på ett kontinuerligt och systematiskt arbete med informations- och cybersäkerhet inom en rad centrala sektorer, krav som på sikt kommer att kompletteras med sektorsspecifika krav från respektive tillsynsmyndighet på att vidta säkerhetsåtgärder. Det finns behov av att etablera förbättrade samverkansformer för de aktörer som omfattas av NIS-regleringen, exempelvis erbjuda praktiska mötesformer och möjligheter att dela kunskap. Vidare är det viktigt att fortsätta öka det stöd som MSB och andra myndigheter lämnar, samt att även se över NIS-regleringens nuvarande tillämpningsområde.

22. Ju2019/03057/SSK

I väntan på att de nya föreskrifterna ska träda i kraft finns det ett stort värde i att åtminstone implementera vissa grundläggande it-säkerhetsåtgärder. Dessa är primärt framtagna för att bemöta antagonistiska hot men flera av åtgärderna skulle även kunna användas för att minska konsekvensen av vanligt förekommande incidenter och för att höja den generella nivån.

- Inaktivera oanvända tjänster och protokoll
- Segmentera nätverken och filtrera trafiken mellan segmenten
- Inför flerfaktorsautentisering för konton med administrativa behörigheter
- Begränsa användningen av administrativa behörigheter
- Konfigurera så att säkerhetsloggar skickas centralt och att dessa analyseras
- Installera säkerhetsuppdateringar så fort det går
- Uppgradera mjuk- och hårdvara samt operativsystem
- Inför att endast godkänd programvara får köras (vitlistning) och inaktivera att makron körs
- Använd antivirus/antimalware
- Konfigurera säkerhetskopiering och testa återställning.

6.2 Arbeta systematiskt och riskbaserat

För att kunna säkerställa en tillräcklig nivå av informationssäkerhet i en organisation är det viktigt att informationssäkerhetsarbetet bedrivs systematiskt, riskbaserat och långsiktigt. Att arbeta på detta sätt bidrar till ett bra säkerhetsarbete som skyddar organisationens informationstillgångar. Det bidrar även till att resurser används till det som är viktigt och att organisationen i samband med en incident kan hantera och även återhämta sig efter händelsen.

MSB:s metodstöd är framtaget för att stötta organisationer i att bedriva ett systematiskt informationssäkerhetsarbete. Metodstödet i sin tur bygger på de internationella standarderna i ISO/IEC 27000serien.

Metodstödet beskriver hur de komponenter som utgör ett ledningssystem för informationssäkerhet (LIS) kan utformas. Ett LIS består av alla de delar som krävs för att kunna skapa en systematik för arbetet med informationssäkerhet – allt från styrande dokument till metodik.

Metodstödet är tillgängligt för alla, och går att applicera oavsett storlek eller organisationsform. Givet problematiken med underrapportering och bristande kontinuitetsplanering är förhoppningen att detta stöd ska höja lägstanivån, samt öka rapporteringsgraden och samtidigt minska konsekvenserna av de inrapporterade incidenterna.

Du hittar metodstödet i sin helhet och fler verktyg på: informationssakerhet.se

Nedan följer ett antal råd och tips på hur en organisation kan arbeta systematiskt med stöd från metodstödet.

- Ledningens ansvar. Ledningen har det övergripande ansvaret för informationssäkerheten inom sin organisation. Den är ytterst ansvarig och behöver fatta nödvändiga beslut om inriktning och resurser samt följa upp att resultat uppfyller ställda förväntningar. En ledning som är engagerad och införstådd med verksamhetsnyttan med informationssäkerhetsarbetet skapar goda förutsättningar för att myndighetens information skyddas tillräckligt.
- Organiseringen av informationssäkerhetsarbetet. För att över tid kunna utveckla och erhålla kontinuitet i informationssäkerhetsarbetet är det väsentligt att roller och ansvar är definierade och kända inom hela organisationen. Det är bättre att ta fram en enkel organisation med medvetet valda arbetssätt till att börja med, roller kan utökas efter hand.
- Internt regelverk. Styrdokument som är underliggande till informationssäkerhetspolicyn, som anvisningar och instruktioner är ofta omfattande och riktar sig till olika målgrupper. De bör därför anpassas för dessa. Håll nere antalet anvisningar och se om du kan föra in instruktioner gällande informationssäkerhet i målgruppernas befintliga dokumentation som beskriver hur de ska utföra olika arbetsuppgifter.
- Identifiera informationstillgångar. Analysera era informationstillgångar – det vill säga information som verksamheten hanterar och som ni därmed ska skydda, inklusive de resurser som behandlar informationen (exempelvis it-system). Kom ihåg att informationstillgångar är inte bara sådana som ”ägs” av organisationen. Externa informationstillgångar som organisationen är beroende av kan vara kritiska liksom informationstillgångar som är gemensamma, t.ex. med samarbetsparters eller systemleverantörer.
- Omvärldsanalys. Analysera organisationens externa intressenter och hur relationen påverkar er informationshantering och i förlängningen informationssäkerheten. Ta stöd av kollegor i branschen/sektorn, gemensamma förbund eller föreningar som har liknande förutsättningar i omvärlden. Använd aktuella beskrivningar av hotbild, exempelvis i trend- och årsrapporter (internationella, nationella och sektorspecifika).

6.2.1 Nytt stöd för uppföljning

MSB har fått i uppdrag av regeringen att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. Det innebär att statliga myndigheter, kommuner och regioner regelbundet ska erbjudas att delta i en uppföljning och få återkoppling om nivån på sitt informationssäkerhetsarbete och vilka förbättringsåtgärder de kan vidta. Uppföljningsstrukturen ska också leda till att MSB kan lämna en samlad nivåbedömning till regeringen och bättre utveckla myndighetens stöd. Viktiga referenspunkter i arbetet med att utveckla uppföljningsstrukturen är bland annat standardserien ISO/IEC 27000 samt MSB:s föreskrifter och stöd på området.

Uppföljningsstrukturen ska vara ett stöd för den offentliga förvaltningen och bidra till organisationernas eget förbättringsarbete och lärande. Olika organisationer har nått olika långt och återkopplingen är tänkt att stödja stegvis utveckling av arbetet. Uppföljningen ska därefter genomföras regelbundet och bli en del av MSB:s löpande verksamhet.

Exempel på angrepp

En myndighet fick in skräppost som passerade e-postfiltret. I meddelandet uppmanades användare att byta lösenord genom att följa en länk. Totalt lurades över 100 användare att lämna ut sina inloggningsuppgifter. En extern aktör utnyttjade sedan e-postkonton hos myndigheten i syfte att skicka skräppost. Kontouppgifterna missbrukades inte på andra sätt enligt den drabbade myndigheten. Genom loggar kunde man spåra vilka användare som anslutit mot den externa webbservern, och på så sätt identifiera kapade konton. Dessa konton inaktiverades och deras respektive lösenord byttes ut.

Så fort myndigheten blev medveten om incidenten blockerades tillgången till den externa sajten. Vidare loggades alla försök att få tillgång till sajten och dessa konton inaktiverades. Myndigheten övervakade också sitt skräppostfilter för att se om några försök att skicka ut skräppost hade gjorts. Efter tre dagar bedömdes det akuta skedet vara över.

Omfattningen av incidenten var att cirka 200 000 skräppostmeddelanden skickades ut från myndighetens e-postserver. En effekt blev att myndigheten fick problem att skicka e-post under två timmar då den blev svartlistad av ett flertal domäner. Den hade också återkommande problem med fördröjning av e-postleverans på grund av den tidigare svartlistningen.

I incidentrapporten framgår även att myndigheten planerade genomföra ett antal utbildningsinsatser för att minska risken att liknande händelser sker igen. Den planerade även att byta sitt e-postfilter samt införa säkerhetshöjande åtgärder på sina e-postservrar.

Rekommendation

Myndigheten har vidtagit ett antal korrekta åtgärder för att förhindra att liknande incidenter sker igen. Förutom informationsinsatser för att utbilda personalen om kända nätfiskemetoder och hur känslig information bör skyddas så rekommenderas en översyn av skyddslösningar och kontrollsystem för att säkerställa att tillräckligt skydd är installerat i alla led i it-miljön.

6.3 Hantera incidenter

När det gäller operativ it-incidenthantering är det funktionen CERT-SE som är Sveriges nationella funktion för hantering av it-relaterade incidenter inom samhällsviktig verksamhet i både privat och offentlig sektor. För att kunna tillhandahålla det bästa möjliga stödet sker internationellt samarbete och omvärldsbevakning gällande bland annat sårbarheter i produkter, skadlig kod, attackmetoder samt intrång och otillåten användning av it-system. Förutom att hantera pågående incidenter omsätter CERT-SE information till rekommendationer och förmedlar till verksamheter i syfte att konkret stödja och förbättra it-säkerheten.

Vid en incident kan CERT-SE stödja med exempelvis rådgivning kring hanteringen, eventuella kopplingar till pågående eller tidigare händelser och teknisk analys av angripna system. För att minska risk för spridning publiceras råd kring utnyttjade sårbarheter och rekommenderade åtgärder. När flera intressenter behöver samverka kan CERT-SE koordinera det arbetet.

CERT-SE kan nås dygnet runt, alla dagar på året.

För att ge bästa möjliga stöd vid en incident är det bra om följande uppgifter finns tillgängliga:

- Vad har hänt?
- Hur och när upptäcktes it-incidenten?
- Vilka åtgärder har vidtagits?
- Är incidenten pågående?
- Kan CERT-SE och MSB hjälpa till? Hur?
- Gör polisanmälan om incidenten har brottslig karaktär.

Exempel på informationsläckage eller -förlust

I samband med en systemuppdatering som genomfördes inför årsskiftet 2018–2019 inträffade en incident där uppgifter röjdes under den givna perioden. Detta uppdagades och rapporterades först under hösten 2019. Incidenten visade att ett antal personers information oavsiktligt ändrades i samband med den tidigare systemhändelsen och risken var att dessa känsliga uppgifter kunde ha röjts. Vid den första analysen bedömde myndigheten att incidenten omfattade personer med skyddade personuppgifter, och att detta var kopplat till den specifika systemhändelsen.

Myndigheten kunde inte hitta några indikationer på att de skyddade uppgifterna hade utnyttjats av obehöriga internt i systemmiljöerna eller vid kontakt med myndigheten.

Rekommendation

Det är viktigt att verifiera att förändringar i it-miljön får det resultat som man förväntat sig. I det här fallet hade lång tid förflutit mellan händelsen och upptäckten av den. Ett sätt att minska risken för att något liknande inträffar är att se över verifieringsrutiner och även se till att det finns någon som är ytterst ansvarig för att förändringarna sker korrekt och fullständigt.

Fokusområden

7. Fokusområden

Nedan följer ett axplock av de områden MSB fokuserat på och kommer att fokusera på för att öka samhällets informations- och cybersäkerhet.

7.1 Behovsinventering

MSB har under 2019 kontaktat de flesta rapporteringsskyldiga myndigheter och gjort en behovsinventering med anledning av deras rapportering, eller frånvaron av den. I korrespondensen ingick en förfrågan om intresset för stöd från MSB gällande systematiskt- och riskbaserat arbete, förebyggande tekniska åtgärder samt operativt stöd från CERT-SE vid hanteringen av händelser. MSB har sammanställt svaren och kommer under 2020 att gå vidare genom att analysera hur man på bästa sätt kan erbjuda ytterligare stöd.

7.2 Samlad informations- och cybersäkerhetshandlingsplan 2019–2022

I juli 2018 gav regeringen MSB, FRA, Försvarets materielverk (FMV), Försvarsmakten, Post- och telestyrelsen (PTS), Polismyndigheten och Säkerhetspolisen i uppdrag att ta fram en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022.

Handlingsplanen bidrar till att ge regeringen ett bättre underlag för att kunna analysera om myndigheternas planerade åtgärder är tillräckliga för att nå målsättningarna i den nationella strategin och vilka ytterligare åtgärder regeringen behöver vidta. Enligt regeringen bör den samlade handlingsplanen syfta till att det sker en samordning avseende myndigheternas åtgärder och aktiviteter.

Samtliga åtgärder i handlingsplanen ansluter till någon eller några av de sex strategiska prioriteringar som regeringen beslutat i den nationella strategin för samhällets informations- och cybersäkerhet.[23] Arbetet med åtgärderna i handlingsplanen ska rapporteras årligen till regeringen den 1 mars.

2020 års redovisning består av 77 åtgärder. Nästan en tredjedel av åtgärderna genomförs i samverkan mellan en eller flera av myndigheterna som ingår i uppdraget och många åtgärder sker i samverkan med andra aktörer i samhället. Mer än hälften av åtgärderna är nya eller uppdaterade jämfört med föregående år. Nytt i 2020 års redovisning är, förutom flera nya åtgärder, nya kapitel om extern samverkan samt uppföljning. Under 2020 kommer även arbetet med handlingsplanen för 2021 att påbörjas.

23. Skr. 2016/17:213

7.3 Nationellt cybersäkerhetscenter

I början av 2019 aviserade regeringen att ett nationellt cybersäkerhetscenter ska inrättas i Sverige. Under hösten samma år fick FRA, Försvarsmakten, MSB och Säkerhetspolisen ett regeringsuppdrag inför inrättandet av ett sådant center. Uppdraget redovisades i samråd med Polismyndigheten, FMV och PTS i december 2019.

Som ett led i fördjupad myndighetssamverkan driver de sju myndigheterna ett gemensamt projekt för att förbereda etablerandet av ett nationellt cybersäkerhetscenter. Projektet pågår under 2020 och ska förutom beredning av centrala frågor även göra de första gemensamma leveranserna.

Myndigheterna är överens om att extern samverkan är en central del av verksamheten i ett framtida nationellt cybersäkerhetscenter. Fullt utbyggt kommer centret att stödja cybersäkerhetsarbetet i en bredd av målgrupper i både privat och offentlig sektor.

7.4 Totalförsvarets behov av informations- och cybersäkerhet

Den återupptagna totalförsvarsplaneringen ställer höga krav på myndigheternas förmåga att hantera och arbeta med information med höga skyddsvärden. Totalförsvarsplaneringen är dimensionerande för informationssäkerhetsarbetet, men det är viktigt att även planera för och ha kapacitet att klara av krissituationer samt lägen vid, eller inför höjd beredskap.

Kopplingen informations- och cybersäkerhet och krisberedskap och planering inför höjd beredskap är stark, och en väl fungerande informationshantering vid såväl kris som i ett läge av höjd beredskap är oerhört viktigt för att klara av krisen, eller kriget. Planeringen inför höjd beredskap är även viktig då den tvingar myndigheter att analysera vilka beroenden de har, dels gentemot andra myndigheter, men även mot den privata sektorn. Energiförsörjning och fungerande telekom är vitala aspekter om något informationsutbyte ska ske mellan statliga myndigheter, eller privata aktörer under kris, eller höjd beredskap. Under 2019 har MSB, tillsammans med PTS arbetat med en områdesvis programplan för området information och kommunikation. Denna programplan är en pilot för att påbörja arbetet med att identifiera och planera för hur området information och kommunikation ser ut, och hänger ihop. Detta arbete har belyst det faktum att stora delar, i princip hela, samhället har ett stort beroende gentemot elektronisk kommunikation och informationsutbyte. Det stora beroendet är sant även under normalläge, samt kris. Arbetet är en viktig medvetandehöjande insats, och detta bör göras tydligt för samtliga aktörer.

Informations- och cybersäkerhet kommer att spela en central roll i den situation som ofta beskrivs som gråzon. Cyberangrepp och fysiska angrepp som påverkar elektronisk kommunikation och informationsutbyte i samhällsviktig verksamhet är troliga i ett gråzonsläge. För att öka beredskapen inför en sådan situation behöver samtliga aktörer förstå sin egen informationshantering och sin roll i det moderna totalförsvaret. MSB arbetar med dessa frågor dels inom ansvarsområdet samhällets informations- och cybersäkerhet, men även gällande Totalförsvarsövning (TFÖ) 2020 som planeras, genomförs och utvärderas gemensamt av MSB och Försvarsmakten.

7.5 Nationellt ramverk för grunddata och digital infrastruktur för informationsutbyte

Sedan hösten 2019 deltar MSB i två regeringsuppdrag med fokus på att främja den digitala utvecklingen av svensk offentlig förvaltnings informationshantering. Uppdragen genomförs av en rad olika centrala myndigheter med Myndigheten för digital förvaltning (DIGG) i ledningen. Genom ett nationellt ramverk för grunddata och en förvaltningsgemensam digital infrastruktur för informationsutbyte ska gemensam hantering och utbyte av information bli mer effektivt och ge ökade möjligheter till styrning och samordning. I och med att myndigheterna går mot att standardisera och bygga ut det förvaltningsgemensamma digitala informationsutbytet blir det extra viktigt att från början etablera ett gemensamt informationssäkerhetsarbete. Den gemensamma informationssäkerheten behöver särskilt dimensioneras och utvecklas i takt med att alltmer komplexa beroendeförhållanden skapas och volymen av information som delas och vidareutnyttjas växer.

MSB är med och stöttar informationssäkerhetsarbetet aktivt i dessa utvecklingsprojekt inom offentlig sektor. Målet är att bidra till en fortsatt säker och hållbar digitalisering. Stödet utformas efter bland anant de lärdomar som görs av dagens it-incidentrapportering.

Utmaningar

8. Utmaningar

Omvärldsutvecklingen går fort framåt när det gäller informationsteknologi vilket ställer höga krav på verksamheter att i ett tidigt stadium, och med en övergripande ansats, arbeta förebyggande, systematiskt och riskbaserat med informations- och cybersäkerhet. Det är tydligt att ingen verksamhet helt kan undvika it-incidenter. Det är också tydligt att många av de incidenter som inträffar får större konsekvenser på grund av ett undermåligt säkerhetsarbete. Detta innebär att många konsekvenser som uppstår, och som på ett eller annat sätt innebär kostnader för verksamheterna skulle ha kunnat minskas/undvikas om det systematiska och det riskbaserade arbetet varit bättre, eller prioriterats av ledningen. Det ska dock tilläggas att det även sker incidenter, med konsekvenser som är oundvikliga, oavsett hur det förebyggande arbetet bedrivits. Den stora skillnaden är att verksamheter och organisationer som arbetar systematiskt och riskbaserat snabbare inser vad som händer, samt mildrar konsekvenserna av incidenterna på ett effektivare sätt än om det görs ad hoc. Denna distinktion är viktig, ingen verksamhet, eller organisation kommer undgå att fortsätta digitaliseras. Denna digitalisering innebär att nya analyser måste göras för att säkerställa att det som behöver skyddas, och det som behöver fungera ges förutsättningar av ledningen att göra det.

Hur myndigheter klarar av att hantera kommande årens teknikskiften kommer att vara avgörande. Ny kommunikationsteknologi i kombination med en exponentiell ökning av uppkopplade produkter samt dramatiskt ökad beräknings- och lagringskapacitet innebär stora förändringar för många myndigheter. Även om verksamheten i sig inte använder någon av dessa har de stor påverkan på samhället i övrigt vilket är något som alla behöver förhålla sig till. Med dessa framsteg kommer nya produkter, möjligheten att erbjuda service på ett annat sätt, samt stora effektiviseringsvinster. Det kan dock vara svårt för organisationer och verksamheter att analysera när en viss ”nymodighet” blivit central i verksamheten. De eventuella säkerhetsproblem eller brister som detta innebär påvisar behovet av löpande översyn av säkerhetsarbetet.

Inget talar för att intensiteten i digitaliseringsarbetet kommer att minska, tvärtom, det kommer förmodligen att drivas på i oförminskad, eller ökad styrka. Denna trend, eller normaltillstånd, behöver införlivas i verksamhetsplaneringar, riskbedömningar, kontinuitetsplaneringar samt, inte minst, i arbetet som sker på ledningsnivå. Givet dessa förutsättningar är det viktigt att det stöd som finns att tillgå används, samt att incidenter rapporteras när de inträffar. Samtliga aktörer, inklusive MSB behöver ta ett helhetsgrepp gällande digitaliseringen och de säkerhetsaspekter som följer med den. Detta för att säkerställa att digitaliseringens fördelar nyttjas fullt ut, utan att riskera medborgarnas förtroende för statens förmåga att med ändamålsenlig säkerhet erbjuda den service som förväntas.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1526 - april 2020 ISBN 978-91-7927-027-8